FIBONACCI PRIMITIVE ROOTS

DANIEL SHANKS
Computation and Mathematics Dept., Naval Ship R & D Center, Washington, D. C.

1. INTRODUCTION

A prime p possesses a Fibonacci Primitive Root g if g is a primitive root of p and if it satisfies

(1) $$g^2 \equiv g + 1 \pmod{p} .$$

It is obvious that if (1) holds then so do

(2) $$g^3 \equiv g^2 + g \pmod{p} ,$$

(3) $$g^4 \equiv g^3 + g^2 \pmod{p} ,$$

etc.

For example, $g = 8$ is one of the four primitive roots of $p = 11$ (the others being 2, 6, 7), and $g = 8$ (only) satisfies (1). Thus, its powers 8^n (mod 11) are

$$1, 8, 9, 6, 4, 10, \cdots \pmod{11}$$

and may be computed not only by

$$9 \equiv 8^2, \quad 6 \equiv 9 \cdot 8, \quad 4 \equiv 9 \cdot 8, \cdots \pmod{11} ,$$

but also, more simply, by

$$9 \equiv 8 + 1, \quad 6 \equiv 9 + 8, \quad 4 \equiv 6 + 9, \cdots \pmod{11} .$$

Thus the name: Fibonacci Primitive Root.

The brief Table 1 shows every $p < 200$ that has an F. P. R., and every such g satisfying $0 < g < p$ that it possesses. By incomplete induction (a

TABLE 1

p	g	p	g
5	3	71	63
11	8	79	30
19	15	109	11, 99
31	13	131	120
41	7, 35	149	41, 109
59	34	179	105
61	18, 44	191	89

fine old expression seldom used these days), we observe the following properties, all of which are easily proved in the next section.

A. Except for the singular $p = 5$, all p having an F. P. R. are $= \pm 1 \pmod{10}$.

B. But not all $p = \pm 1 \pmod{10}$ have an F. P. R., since, e. g., $p = 29$ and 101 do not.

C. Except for the singular $p = 5$, the number of g in $0 < g < p$, if any, is 1 or 2 according as $p \equiv -1$ or $+1 \pmod 4$.

D. In the latter case, the two g satisfy

$$g_1 + g_2 = p + 1 . \tag{4}$$

2. ELEMENTARY PROPERTIES

The solutions of (1) are

$$g = (1 \pm \sqrt{5})2^{-1} \qquad \pmod p \tag{5}$$

and therefore exist if, and only if, $p = 5$, $g = 3$, or $p = 10k \pm 1$, since only these p have 5 as a quadratic residue. This proves A. For $p = 29$, the two solutions of (1) are $g = 6$ and 24, but since these are also quadratic residues of 29, they cannot be primitive roots, thus proving B. The product of the two solutions (5) is given by

(6) $$g_1 g_2 \equiv -1 \pmod{p} .$$

Thus, if $p \equiv -1 \pmod 4$, one g is a quadratic residue and one g is not. There can, therefore, then be at most one F. P. R. On the other hand, for $p \equiv +1 \pmod 4$, consider

$$g_2 \equiv -g_1^{-1} .$$

If g_1 is primitive, and g_2 is of order m, then

$$g_1^m \equiv (-1)^m .$$

Therefore, m is even, and so g_2 is primitive also. Thus, g_1 and g_2 are both primitive, or neither is. This completes C. Finally,

(7) $$g_1 + g_2 \equiv 1 \pmod{p}$$

and (4) follows from $0 < g < p$.

3. THE ASYMPTOTIC DENSITY

Let $F(x)$ be the number of primes $p \le x$ having an F. P. R. (We do not distinguish in this count whether p has one or two.) Then with $\pi(x)$ being the total number of primes $\le x$, we

Conjecture: As $x \to \infty$,

(8) $$\frac{F(x)}{(x)} \sim \frac{27A}{38} = 0.2657054465 \cdots ,$$

where

(9) $$A = \prod_{p=2}^{\infty} \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136 \cdots$$

is Artin's constant.

Artin originally conjectured, cf. [1], [2, page 81] that if $\nu_a(x)$ is the number of $p \le x$ having a as a primitive root, and if

$$a \neq b^n \qquad (n > 1) ,$$

then

$$\frac{\nu_a(x)}{\pi(x)} \sim A . \tag{10}$$

Subsequently, [3] it was found that the heuristic argument was faulty for a = 5, -3, and infinitely many other a but it was still considered reasonable for a = 2, 3, 6, 7, 10, etc. Both heuristically and empirically, Eq. (10) seems correct for these a, and Hooley [4] recently proved that (10) is then true provided one assumes a sufficient number of Riemann Hypotheses.

The heuristic argument for (8) is similar to that which leads to (10), but we must modify two of the factors in (9). Consider the primes in the eight residue classes

$$20k + 1, 3, 7, 9, 11, 13, 17, 19 .$$

Those in 20k + 3, 7, 13, 17 cannot have an F.P.R. For those in 20k + 11, 19 the factor

$$1 - \frac{1}{2(2 - 1)}$$

in (9) must be deleted. This represented the probability that a is not a quadratic residue and therefore could be a primitive root. But for 20k + 11, 19, one of g_1 and g_2 must always be a quadratic nonresidue as we have shown with (6). The factor

$$1 - \frac{1}{5(5 - 1)}$$

in (9) represented the probability that a is not a quintic residue and therefore could be a primitive root. For $20k + 9$, 19 p has no quintic residues since these p are not $\equiv 1 \pmod 5$, and so this factor is deleted. For $20k + 1$, 11, p is always $\equiv 1 \pmod 5$, and the factor must be changed to

$$1 - \frac{1}{5} .$$

Therefore, the expected density of p in these eight residue classes having an F. P. R. is the following:

$20k + 1$	$16A/19$	$20k + 11$	$32A/19$
$20k + 3$	0	$20k + 13$	0
$20k + 7$	0	$20k + 17$	0
$20k + 9$	$20A/19$	$20k + 19$	$40A/19$

As $x \to \infty$, the eight classes of primes are equinumerous, and so (8) follows from this table by averaging these densities. On the other hand, it is known that the number of primes in

$$20k + 1, \qquad 20k + 9$$

will generally lag somewhat behind the other six classes since 1 and 9 are quadratic residues of 20, cf. [5]. We therefore expect that the convergence of $F(x)/\pi(x)$ to $27A/38$ will be mostly from above.

The empirical facts are given in Table 2.

TABLE 2

x	F(x)	(x)	F(x)/π(x)
500	31	95	0.3263
1000	46	168	0.2738
1500	66	239	0.2762
2000	81	303	0.2673
2500	97	367	0.2643

This seems thoroughly satisfactory.

It seems likely that one could transcribe Hooley's theory [4] to the present variant, and thereby prove (8), assuming a sufficient number of Riemann Hypotheses. But the theory in [4] is by no means simple, and this transcription has not been attempted so far.

4. SEVERAL REFERENCES

In closing, we indicate three references related to the concept developed here. The idea for a Fibonacci Primitive Root was suggested by Exercise 158 in [2, page 206]. It is shown there that if g is <u>any</u> primitive root of <u>any</u> prime p, the sequence of first differences

$$g^{n+1} - g^n \pmod{p} \tag{11}$$

is the same as the sequence

$$g^{n-d} \pmod{p} \tag{12}$$

for some fixed displacement d. If, now, one has the first d powers of g:

$$1,\ g,\ g^2,\ \cdots,\ g^d\ ,$$

one can obtain all further powers <u>additively</u> from (11). Our construction here forces $d = 1$ and therefore allows this additive computation <u>ab initio</u>.

In [6], W. Schooling gives a curious method of computing logarithms based on the fact that all powers of

$$\varphi = (1 + \sqrt{5})/2$$

can be computed additively:

$$\varphi^2 = \varphi + 1\ ,$$

$$\varphi^3 = \varphi^2 + \varphi\ ,$$

[Continued on page 181.]